Please type a plus sign (+) inside this box → [+]

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# UTILITY PATENT APPLICATION TRANSMITTAL

*(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))*

| | |
|---|---|
| *Attorney Docket No.* | 520.39632X00 |
| *First Inventor or Application Identifier* | Soichi FURUYA |
| *Title* | See 1 in Addendum |
| *Express Mail Label No.* | |



## APPLICATION ELEMENTS

*See MPEP chapter 600 concerning utility patent application contents.*

*ADDRESS TO:* Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231

1. [X] * Fee Transmittal Form *(e.g., PTO/SB/17)* *(Submit an original and a duplicate for fee processing)*
2. [X] Specification [*Total Pages* 80 ] *(preferred arrangement set forth below)*
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
3. [X] Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 34 ]
4. Oath or Declaration [*Total Pages* 5 ]
   - a. [X] Newly executed (original or copy)
   - b. [ ] Copy from a prior application (37 C.F.R. § 1.63(d)) *(for continuation/divisional with Box 16 completed)*
     - i. [ ] DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

** NOTE FOR ITEMS 1 & 13 IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).*

5. [ ] Microfiche Computer Program *(Appendix)*
6. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   - a. [ ] Computer Readable Copy
   - b. [ ] Paper Copy (identical to computer copy)
   - c. [ ] Statement verifying identity of above copies

## ACCOMPANYING APPLICATION PARTS

7. [X] Assignment Papers (cover sheet & document(s))
8. [ ] 37 C.F.R.§3.73(b) Statement *(when there is an assignee)* [X] Power of Attorney
9. [ ] English Translation Document *(if applicable)*
10. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
11. [ ] Preliminary Amendment
12. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
13. [ ] * Small Entity Statement(s) *(PTO/SB/09-12)* [ ] Statement filed in prior application Status still proper and desired
14. [X] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
15. [X] Other: See 2 in Addendum

16. **If a CONTINUING APPLICATION,** *check appropriate box, and supply the requisite information below and in a preliminary amendment:*

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No: _____/_____

*Prior application information:* Examiner _____ *Group / Art Unit:* _____

**For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.**

## 17. CORRESPONDENCE ADDRESS

[X] *Customer Number or Bar Code Label* 020457 *(Insert Customer No. or Attach bar code label here)* *or* [ ] *Correspondence address below*

| | | | | | |
|---|---|---|---|---|---|
| *Name* | | | | | |
| *Address* | | | | | |
| *City* | | *State* | | *Zip Code* | |
| *Country* | | *Telephone* | | *Fax* | |

| | | | |
|---|---|---|---|
| *Name (Print/Type)* | Carl B. Brundidge | *Registration No. (Attorney/Agent)* | 29,621 |
| *Signature* | | *Date* | 02/16/01 |

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

# Attachment to PTO/SB/05 (4/98) Utility Patent Application Transmittal

1. METHOD AND APPARATUS FOR SYMMETRIC-KEY ENCRYPTION
2. - LIST AND COPIES OF PRIOR ART W/REFS.
   - FIGS. 1-39
   - CREDIT CARD PAYMENT FORM

PTO/SB/17 (12/99)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# FEE TRANSMITTAL for FY 2000

*Patent fees are subject to annual revision.*
*Small Entity payments must be supported by a small entity statement, otherwise large entity fees must be paid. See Forms PTO/SB/09-12. See 37 C.F.R. §§ 1.27 and 1.28.*

**TOTAL AMOUNT OF PAYMENT** ($) 1,376.00

| *Complete if Known* | |
|---|---|
| Application Number | |
| Filing Date | February 16, 2001 |
| First Named Inventor | Soichi FURUYA |
| Examiner Name | |
| Group / Art Unit | |
| Attorney Docket No. | 520.39632X00 |

## METHOD OF PAYMENT (check one)

1. ☐ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number: 01-2135

Deposit Account Name: Antonelli,Terry,Stout&Kraus,LLP

☒ Charge Any Additional Fee Required Under 37 CFR §§ 1.16 and 1.17

2. ☒ **Payment Enclosed:** ☐ Check ☐ Money Order ☒ Other

## FEE CALCULATION

### 1. BASIC FILING FEE

| Large Entity Fee Code | Large Entity Fee ($) | Small Entity Fee Code | Small Entity Fee ($) | Fee Description | Fee Paid |
|---|---|---|---|---|---|
| 101 | 690 | 201 | 345 | Utility filing fee | 710.00 |
| 106 | 310 | 206 | 155 | Design filing fee | |
| 107 | 480 | 207 | 240 | Plant filing fee | |
| 108 | 690 | 208 | 345 | Reissue filing fee | |
| 114 | 150 | 214 | 75 | Provisional filing fee | |

SUBTOTAL (1) ($) 710.00

### 2. EXTRA CLAIM FEES

| | | Extra Claims | | Fee from below | Fee Paid |
|---|---|---|---|---|---|
| Total Claims | 37 | -20** = 17 | x | 18 | = 306 |
| Independent Claims | 7 | - 3** = 4 | x | 80 | = 320 |
| Multiple Dependent | | | | | = 0 |

**or number previously paid, if greater; For Reissues, see below

| Large Entity Fee Code | Large Entity Fee ($) | Small Entity Fee Code | Small Entity Fee ($) | Fee Description |
|---|---|---|---|---|
| 103 | 18 | 203 | 9 | Claims in excess of 20 |
| 102 | 78 | 202 | 39 | Independent claims in excess of 3 |
| 104 | 260 | 204 | 130 | Multiple dependent claim, if not paid |
| 109 | 78 | 209 | 39 | ** Reissue independent claims over original patent |
| 110 | 18 | 210 | 9 | ** Reissue claims in excess of 20 and over original patent |

SUBTOTAL (2) ($) 626.00

## FEE CALCULATION (continued)

### 3. ADDITIONAL FEES

| Large Entity Fee Code | Large Entity Fee ($) | Small Entity Fee Code | Small Entity Fee ($) | Fee Description | Fee Paid |
|---|---|---|---|---|---|
| 105 | 130 | 205 | 65 | Surcharge - late filing fee or oath | 0.00 |
| 127 | 50 | 227 | 25 | Surcharge - late provisional filing fee or cover sheet. | 0.00 |
| 139 | 130 | 139 | 130 | Non-English specification | 0.00 |
| 147 | 2,520 | 147 | 2,520 | For filing a request for reexamination | 0.00 |
| 112 | 920* | 112 | 920* | Requesting publication of SIR prior to Examiner action | 0.00 |
| 113 | 1,840* | 113 | 1,840* | Requesting publication of SIR after Examiner action | 0.00 |
| 115 | 110 | 215 | 55 | Extension for reply within first month | 0.00 |
| 116 | 380 | 216 | 190 | Extension for reply within second month | 0.00 |
| 117 | 870 | 217 | 435 | Extension for reply within third month | 0.00 |
| 118 | 1,360 | 218 | 680 | Extension for reply within fourth month | 0.00 |
| 128 | 1,850 | 228 | 925 | Extension for reply within fifth month | 0.00 |
| 119 | 300 | 219 | 150 | Notice of Appeal | 0.00 |
| 120 | 300 | 220 | 150 | Filing a brief in support of an appeal | 0.00 |
| 121 | 260 | 221 | 130 | Request for oral hearing | 0.00 |
| 138 | 1,510 | 138 | 1,510 | Petition to institute a public use proceeding | 0.00 |
| 140 | 110 | 240 | 55 | Petition to revive - unavoidable | 0.00 |
| 141 | 1,210 | 241 | 605 | Petition to revive - unintentional | 0.00 |
| 142 | 1,210 | 242 | 605 | Utility issue fee (or reissue) | 0.00 |
| 143 | 430 | 243 | 215 | Design issue fee | 0.00 |
| 144 | 580 | 244 | 290 | Plant issue fee | 0.00 |
| 122 | 130 | 122 | 130 | Petitions to the Commissioner | 0.00 |
| 123 | 50 | 123 | 50 | Petitions related to provisional applications | 0.00 |
| 126 | 240 | 126 | 240 | Submission of Information Disclosure Stmt | 0.00 |
| 581 | 40 | 581 | 40 | Recording each patent assignment per property (times number of properties) | 40.00 |
| 146 | 690 | 246 | 345 | Filing a submission after final rejection (37 CFR § 1.129(a)) | 0.00 |
| 149 | 690 | 249 | 345 | For each additional invention to be examined (37 CFR § 1.129(b)) | 0.00 |
| Other fee (specify) _____ | | | | | 0.00 |
| Other fee (specify) _____ | | | | | 0.00 |

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 40.00

| SUBMITTED BY | | | | Complete (if applicable) | |
|---|---|---|---|---|---|
| Name (Print/Type) | Carl L. Brundidge | Registration No. (Attorney/Agent) | 29,621 | Telephone | |
| Signature | | | | Date | 02/16/01 |

**WARNING:**

**Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

**For : The Patent Application** **Our Ref. :NT0226US**

- LIST OF THE PRIOR ART REFERENCES CITED IN THE SPECIFICATION

1. Advances in Cryptology-CRYPTO etc.

2. The Chain & Sum Primitive and Its Applications to MACs
   And Stream Ciphers
   Mariusz H. Jakubowski and Ramarathnam Venkatesan
   (281-293)
   "Advances in Cryptology CRYPTO'98" Kaisa Nyberg(Ed.)

3. Keying Hash Functions for Message Authentication
   Mihir Bellare and Ran Canetti and Hugo Krawczyk (1-328)
"Advances in Cryptology CRYPTO'96" Neal Koblitz (Ed.)

4. An Integrity Check Value Algorithm for Stream Ciphers
   Richard Taylor (40-48)
"Advances in Cryptology CRYPTO'93" Douglas R.Stinson (Ed.)

5. Algorithm Types and Modes (189-401)

6. UMAC: Fast and Secure Message Authentication
   J.Black, S.Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway
  (pg.216-269)
"Advances in Cryptology CRYPTO'99" Michael Wiener (Ed.)

7. MMH: Software Message Authentication in the Gbit/Second
   Rates Shai Halevi and Hugo Krawczyk (172-189)
"Fast Software Encryption" Eli Biham (Ed.)

8. Integrity-Aware PCBC Encryption Schemes
   Virgil D Gligor, Pompiliu Donescu (1-13)
"The 1999 Security Protocols Workshop Pre-proceedings"

9. Stream ciphers based on LFSRs (203-369)

Reference


| | | | | |
|---|---|---|---|---|
| Richard Taylor | An Integrity Check Value Algorithm for Stream | pp.40-48 | LNCS773 | CRYPTO93 |
| Mihir Bellare<br>Ran Canetti<br>Hugo Krawczyk | Keying Hash Functions for Message Authentication | pp.1-15 | | CRYPTO96 |
| M. Atici<br>D. R. Stinson | Universal Hashing and Multiple Authenitcation | pp.16-30 | LNCS1109 | CRYPTO96 |
| Tor Helleseth<br>Thomas Johansson | Universal Hash Functions from Exponential Sums over Finite Fields and | pp.31-44 | LNCS1109 | CRYPTO96 |
| Victor Shoup | On Fast and Provably Secure Message | pp.313-328 | LNCS1109 | CRYPTO96 |
| Mariusz H. Jakubowski<br>Ramarathnam<br>Venkatesan | Authentication Based on The Chain & Sum Primitive and Its Applications to MACs and Stream Ciphers | pp.281-293 | LNCS1403 | EUROCRYPT98 |
| J Black<br>S. Halevi<br>H. Krawczyk<br>T. Krovetz<br>P. Rogaway | UMAC: Fast and Secure Message Authentication | pp.216-233 | LNCS1666 | CRYPTO99 |
| Mark Etzel<br>Sarvar Patel<br>Zulfikar Ramzan | Square Hash: Fast Message Authentication via Optimized Universal Hash | pp.234-251 | LNCS1666 | CRYPTO99 |
| Jee Hea An<br>Mihir Bellare | Constructing VIL-MACs from FIL-MACs: Message Authentication under Weakened Assumptions | pp.252-269 | LNCS1666 | CRYPTO99 |
| Shai Halevi<br>Hugo Krawczyk | MMH: Software Message Authentication in the Gbit/Second Rates | pp.172-189 | LNCS1267 | FSE97 |
| Virgil D. Gligor<br>Pompiliu Donescu | Integrity-Aware PCBC Encryption Schemes | | The 1999 Security Protocols Workshop Pre-proceedings, Cambridge UK, 1999. | |
| Alfred J. Menezes<br>Paul C. van Oorschot<br>Scott A. Vanstone | Handbook of Applied Cryptography | pp.203-212, 250-259, 263-266, 347-349, 352- | ISBN0-8493-8523-7 | |
| Bruce Schneier | Applied Cryptography, second edition | pp.189-209, 398- | ISBN0-471-11709-9 | |